Available online at www.sciencedirect.com

ScienceDirect

Journal of Algebra 314 (2007) 888–894

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Subspaces of computable vector spaces ☆

Rodney G. Downey [a], Denis R. Hirschfeldt [b], Asher M. Kach [c], Steffen Lempp [c,*], Joseph R. Mileti [b], Antonio Montalbán [b]

[a] *Department of Mathematics, Victoria University, PO Box 600, Wellington, New Zealand*
[b] *Department of Mathematics, University of Chicago, Chicago, IL 60637-1514, USA*
[c] *Department of Mathematics, University of Wisconsin, Madison, WI 53706-1388, USA*

Received 16 June 2006

Available online 27 April 2007

Communicated by Efim Zelmanov

Abstract

We show that the existence of a nontrivial proper subspace of a vector space of dimension greater than one (over an infinite field) is equivalent to WKL_0 over RCA_0, and that the existence of a finite-dimensional nontrivial proper subspace of such a vector space is equivalent to ACA_0 over RCA_0.

Keywords: Computable vector space; Reverse mathematics; Subspace

1. Introduction

This paper is a continuation of [3], which is a paper by three of the authors of the present paper. In [3], the effective content of the theory of ideals in commutative rings was studied; in particular, the following computability-theoretic results were established:

☆ The first author's research was partially supported by The Marsden Fund of New Zealand. The second author's research was partially supported by NSF grant DMS-0500590. The third author's research was partially supported by a VIGRE grant fellowship. The fourth author's research was partially supported by NSF grant DMS-0140120. The fifth author's research was partially supported by NSF grant DMS-0502215. The sixth author's research was partially supported by NSF grant DMS-0600824.
* Corresponding author.

E-mail addresses: rod.downey@mcs.vuw.ac.nz (R.G. Downey), drh@math.uchicago.edu (D.R. Hirschfeldt), kach@math.wisc.edu (A.M. Kach), lempp@math.wisc.edu (S. Lempp), mileti@math.uchicago.edu (J.R. Mileti), antonio@math.uchicago.edu (A. Montalbán).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.08.040

Theorem 1.1.

(1) *There exists a computable integral domain R that is not a field such that* $\deg(I) \gg \mathbf{0}$ *for all nontrivial proper ideals I of R.*
(2) *There exists a computable integral domain R that is not a field such that* $\deg(I) = \mathbf{0}'$ *for all finitely generated nontrivial proper ideals I of R.*

These results immediately gave the following proof-theoretic corollaries:

Corollary 1.2.

(1) *Over* RCA_0, WKL_0 *is equivalent to the statement* "*Every* (*infinite*) *commutative ring with identity that is not a field has a nontrivial proper ideal.*"
(2) *Over* RCA_0, ACA_0 *is equivalent to the statement* "*Every* (*infinite*) *commutative ring with identity that is not a field has a finitely generated nontrivial proper ideal.*"

In the present paper, we complement these results with related results from linear algebra. (We refer to [3] for background, motivation, and definitions.)

We start with the following

Definition 1.3.

(1) A *computable field* is a computable subset $F \subseteq \mathbb{N}$ equipped with two computable binary operations $+$ and $\cdot$ on F, together with two elements $0, 1 \in F$ such that $(F, 0, 1, +, \cdot)$ is a field.
(2) A *computable vector space* (over a computable field F) is a computable subset $V \subseteq \mathbb{N}$ equipped with two computable operations $+ : V^2 \to V$ and $\cdot : F \times V \to V$, together with an element $0 \in V$ such that $(V, 0, +, \cdot)$ is a vector space over F.

This notion was first studied by Dekker [2], then more systematically by Metakides and Nerode [4] and many others.

As in [3] for nontrivial proper ideals in rings, one motivation in the results below is to understand the complexity of nontrivial proper subspaces of a vector space of dimension greater than one, and the proof-theoretic axioms needed to establish their existence. For example, consider the following elementary characterization of when a vector space has dimension greater than one.

Proposition 1.4. *A vector space V has dimension greater than one if and only if it has a nontrivial proper subspace.*

As in the case of ideals in [3], we will be able to show that this equivalence is not effective, and to pin down the exact proof-theoretic strength of the statement in two versions, for the existence of a nontrivial proper subspace and of a finite-dimensional nontrivial proper subspace:

Theorem 1.5.

(1) *There exists a computable vector space V of dimension greater than one* (*over an infinite computable field*) *such that* $\deg(W) \gg \mathbf{0}$ *for all nontrivial proper subspaces W of V.*

(2) *There exists a computable vector space V of dimension greater than one* (*over an infinite computable field*) *such that* $\deg(W) \geqslant \mathbf{0}'$ *for all finite-dimensional nontrivial proper subspaces W of V.*

Again, after a brief analysis of the induction needed to establish Theorem 1.5, we obtain the following proof-theoretic corollaries:

Corollary 1.6.

(1) *Over* RCA_0, WKL_0 *is equivalent to the statement* "*Every vector space of dimension greater than one* (*over an infinite field*) *has a nontrivial proper subspace.*"
(2) *Over* RCA_0, ACA_0 *is equivalent to the statement* "*Every vector space of dimension greater than one* (*over an infinite field*) *has a finite-dimensional nontrivial proper subspace.*"

2. The proof of Theorem 1.5

For the proof of part (1) of Theorem 1.5, we begin with a few easy lemmas:

Lemma 2.1. *Suppose that V is a vector space, that $\{v, w\}$ is a linearly independent set of vectors in V, and that $u \neq 0$ is a vector in V. Then there exists at most one scalar λ such that $u \in \langle v - \lambda w\rangle$.*

Proof. Suppose that $u \in \langle v - \lambda_1 w\rangle$ and that $u \in \langle v - \lambda_2 w\rangle$. Fix μ_1, μ_2 such that $u = \mu_1(v - \lambda_1 w)$ and $u = \mu_2(v - \lambda_2 w)$. Notice that $\mu_1, \mu_2 \neq 0$ because $u \neq 0$. We now have

$$\mu_1 v - \mu_1\lambda_1 w = u = \mu_2 v - \mu_2\lambda_2 w,$$

and hence

$$(\mu_1 - \mu_2)v + (\mu_2\lambda_2 - \mu_1\lambda_1)w = 0.$$

Since $\{v, w\}$ is linearly independent, it follows that $\mu_1 - \mu_2 = 0$ and $\mu_2\lambda_2 - \mu_1\lambda_1 = 0$, hence $\mu_1 = \mu_2$ and $\mu_1\lambda_1 = \mu_2\lambda_2$. Since $\mu_1 = \mu_2 \neq 0$, it follows from the second equation that $\lambda_1 = \lambda_2$. □

Lemma 2.2. *Suppose that V is a vector space with basis B, which is linearly ordered by $\prec$. Suppose that*

(1) $v \in V$.
(2) $e \in B$.
(3) *λ is a scalar.*
(4) $e \succ \max(\mathrm{supp}(v))$ (*where* $\mathrm{supp}(v) = \mathrm{supp}_B(v)$, *the* support *of v, is the finite set of basis vectors in B needed to write v as a linear combination in this basis*).

Then $B \setminus \{e\}$ is a basis for V over $\langle e - \lambda v\rangle$, and, for all $w \in V$, $\max(\mathrm{supp}_{B\setminus\{e\}}(w + \langle e - \lambda v\rangle)) \preccurlyeq \max(\mathrm{supp}_B(w))$.

Proof. Notice that $e \in \langle (B \setminus \{e\}) \cup \{e - \lambda v\} \rangle$ because $e \notin \operatorname{supp}(v)$, so $(B \setminus \{e\}) \cup \{e - \lambda v\}$ spans V. Suppose that $e_1, e_2, \ldots, e_n \in B \setminus \{e\}$ are distinct and $\mu_1, \mu_2, \ldots, \mu_n$ are scalars such that

$$\mu_1 e_1 + \mu_2 e_2 + \cdots + \mu_n e_n \in \langle e - \lambda v \rangle.$$

Fix μ such that

$$\mu_1 e_1 + \mu_2 e_2 + \cdots + \mu_n e_n = \mu(e - \lambda v)$$

and notice that we must have $\mu = 0$ (by looking at the coefficient of e), hence each $\mu_i = 0$ because B is a basis. Therefore, $B \setminus \{e\}$ is a basis for V over $\langle e - \lambda v \rangle$. By hypothesis (4), the last line of the lemma now follows easily. □

Lemma 2.3. *Suppose that V is a vector space with basis B, which is linearly ordered by $\prec$. Suppose that*

(1) $v_1, v_2 \in V$.
(2) $e_1, e_2 \in B$ *with* $e_1 \neq e_2$.
(3) λ *is a scalar.*
(4) $e_1 \succ \max(\operatorname{supp}(v_1) \cup \operatorname{supp}(v_2))$.
(5) $\{v_1, e_1\}$ *is linearly independent.*
(6) $v_1 \notin \langle e_2 - \lambda v_2 \rangle$.

Then $\{v_1, e_1\}$ is linearly independent over $\langle e_2 - \lambda v_2 \rangle$.

Proof. Suppose that

$$\mu_1 v_1 + \mu_2 e_1 = \mu_3(e_2 - \lambda v_2).$$

We need to show that $\mu_1 = \mu_2 = 0$.

Case 1. $e_1 \prec e_2$. In this case, we must have $\mu_3 = 0$ (by looking at the coefficient of e_2). Thus, $\mu_1 v_1 + \mu_2 e_1 = 0$, and hence $\mu_1 = \mu_2 = 0$ since $\{v_1, e_1\}$ is linearly independent.

Case 2. $e_1 \succ e_2$. In this case, we must have $\mu_2 = 0$ (by looking at the coefficient of e_1). Thus, $\mu_1 v_1 = \mu_3(e_2 - \lambda v_2)$. Since $v_1 \notin \langle e_2 - \lambda v_2 \rangle$, this implies that $\mu_1 = 0$. □

By applying the above three lemmas in the corresponding quotient, we obtain the following results.

Lemma 2.4. *Suppose that V is a vector space, that $X \subseteq V$, that $\{v, w\}$ is linearly independent over $\langle X \rangle$, and that $u \notin \langle X \rangle$. Then there exists at most one λ such that $u \in \langle X \cup \{v - \lambda w\} \rangle$.*

Lemma 2.5. *Suppose that V is a vector space, that $X \subseteq V$, and that B is a basis for V over $\langle X \rangle$ that is linearly ordered by $\prec$. Suppose that*

(1) $v \in V$.
(2) $e \in B$.

(3) *λ is a scalar.*
(4) $e \succ \max(\mathrm{supp}(v))$.

Then $B \setminus \{e\}$ is a basis for V over $\langle X \cup \{e - \lambda v\}\rangle$ and, for all $w \in V$, $\max(\mathrm{supp}_{B\setminus\{e\}}(w + \langle X \cup \{e - \lambda v\}\rangle)) \preccurlyeq \max(\mathrm{supp}_B(w))$.

Lemma 2.6. *Suppose that V is a vector space, that $X \subseteq V$, and that B is a basis for V over $\langle X\rangle$ that is linearly ordered by $\prec$. Suppose that*

(1) $v_1, v_2 \in V$.
(2) $e_1, e_2 \in B$ *with* $e_1 \neq e_2$.
(3) *λ is a scalar.*
(4) $e_1 \succ \max(\mathrm{supp}(v_1) \cup \mathrm{supp}(v_2))$.
(5) $\{v_1, e_1\}$ *is linearly independent over* $\langle X\rangle$.
(6) $v_1 \notin \langle X \cup \{e_2 - \lambda v_2\}\rangle$.

Then $\{v_1, e_1\}$ is linearly independent over $\langle X \cup \{e_2 - \lambda v_2\}\rangle$.

Proof of Theorem 1.5. Fix two disjoint c.e. sets A and B such that $\deg(S) \gg \mathbf{0}$ for any set S satisfying $A \subseteq S$ and $B \cap S = \emptyset$. Let V^∞ be the vector space over the infinite computable field F on the basis $e_0, e_1, e_2, \ldots$ (ordered by $\prec$ as listed) and list V^∞ as $v_0, v_1, v_2, \ldots$ (viewed as being coded effectively by natural numbers). We may assume that v_0 is the zero vector of V^∞. Fix a computable injective function $g : \mathbb{N}^3 \to \mathbb{N}$ such that $e_{g(i,j,n)} \succ \max(\mathrm{supp}(v_i) \cup \mathrm{supp}(v_j))$ for all $i, j, n \in \mathbb{N}$. We build a computable subspace U of V^∞ with the plan of taking the quotient $V = V^\infty/U$.

We have the following requirements for all $v_i, v_j \notin U$:

$$\begin{aligned} R_{i,j,n}\colon\ n \notin A \cup B \quad &\Rightarrow \quad \text{each of } \{v_i, e_{g(i,j,n)}\} \text{ and } \{v_j, e_{g(i,j,n)}\} \text{ are linearly independent over } U,\\ n \in A \quad &\Rightarrow \quad e_{g(i,j,n)} - \lambda v_i \in U \text{ for some nonzero } \lambda \in F, \quad \text{and}\\ n \in B \quad &\Rightarrow \quad e_{g(i,j,n)} - \lambda v_j \in U \text{ for some nonzero } \lambda \in F. \end{aligned}$$

We now effectively build a sequence $U_2, U_3, U_4, \ldots$ of finite subsets of V^∞ such that $U_2 \subseteq U_3 \subseteq U_4 \subseteq \cdots$, and we set $U = \bigcup_{n \geqslant 2} U_n$. We also define a function $h : \mathbb{N}^4 \to \{0, 1\}$ for which $h(i, j, n, s) = 1$ if and only if we have acted for requirement $R_{i,j,n}$ at some stage $\leqslant s$ (as defined below). We ensure that for all $k \geqslant 2$, we have $v_k \in U$ if and only if $v_k \in U_k$, which will make our set U computable. We begin by letting $U_2 = \{v_0\}$ and letting $h(i, j, n, s) = 0$ for all i, j, n, s with $s \leqslant 2$. Suppose that $s \geqslant 2$ and we have defined U_s and $h(i, j, n, s)$ for all i, j, n. Suppose also that we have for any i, j, n, and s such that $v_i, v_j \notin \langle U_s\rangle$:

(1) If $h(i, j, n, s) = 0$, then each of $\{v_i, e_{g(i,j,n)}\}$ and $\{v_j, e_{g(i,j,n)}\}$ is linearly independent over $\langle U_s\rangle$.
(2) If $h(i, j, n, s) = 1$ and $n \in A_s$, then $e_{g(i,j,n)} - \lambda v_i \in U_s$ for some nonzero $\lambda \in F$.
(3) If $h(i, j, n, s) = 1$ and $n \in B_s$, then $e_{g(i,j,n)} - \lambda v_j \in U_s$ for some nonzero $\lambda \in F$.

Check whether there exists a triple $\langle i, j, n\rangle < s$ (under some effective coding) such that

(1) $v_i, v_j \notin \langle U_s \rangle$.
(2) $n \in A_s \cup B_s$.
(3) $h(i, j, n, s) = 0$.

Suppose first that no such triple $\langle i, j, n \rangle$ exists. If $v_{s+1} \in \langle U_s \rangle$, then let $U_{s+1} = U_s \cup \{v_{s+1}\}$, otherwise let $U_{s+1} = U_s$. Also, let $h(i, j, n, s+1) = h(i, j, n, s)$ for all i, j, n.

Suppose then that such a triple $\langle i, j, n \rangle$ exists, and fix the least such triple. If $n \in A_s$, then search for the least (under some effective coding) nonzero $\lambda \in F$ such that $v_k \notin \langle U_s \cup \{e_{g(i,j,n)} - \lambda v_i\} \rangle$ for all $k \leqslant s$ such that $v_k \notin U_s$. (Such λ must exist by Lemma 2.4 and the fact that F is infinite.) Let $U'_s = U_s \cup \{e_{g(i,j,n)} - \lambda v_i\}$ and let $h(i, j, n, s+1) = 1$. If $n \in B_s$, then proceed likewise with v_j replacing v_i. Now, if $v_{s+1} \in \langle U'_s \rangle$, then let $U_{s+1} = U'_s \cup \{v_{s+1}\}$; otherwise let $U_{s+1} = U'_s$. Also, let $h(i, j, n, s+1) = h(i, j, n, s)$ for all other i, j, n. Using Lemma 2.6, it follows that our inductive hypothesis is maintained, so we may continue.

We can now view the quotient space $V = V^\infty / U$ as the set of $<_{\mathbb{N}}$-least representatives (which is a computable subset of V^∞). Notice that V is not one-dimensional because $\{v_1, e_{g(1,2,n)}\}$ is linearly independent over U for any $n \notin A \cup B$ (since $v_1, v_2 \notin U$). Suppose that W is a nontrivial proper subspace of V, and fix W_0 such that $W = W_0/U$. Then W_0 is a W-computable subspace of V^∞, and $U \subset W_0 \subset V^\infty$. Fix $v_i, v_j \in V^\infty \setminus U$ such that $v_i \in W_0$ and $v_j \notin W_0$. Let $S = \{n\colon\ e_{g(i,j,n)} \in W_0\}$. We then have that $S \leqslant_T W_0 \equiv_T W$, that $A \subseteq S$, and that $B \cap S = \emptyset$. Thus $\deg(S) \gg \mathbf{0}$, establishing part (1) of Theorem 1.5.

Part (2) of Theorem 1.5 now follows easily from part (1) and Arslanov's Completeness Criterion [1]: If W is a finite-dimensional nontrivial proper subspace of the above vector space V then W_0 is a c.e. set that computes a degree $\gg \mathbf{0}$; thus $\deg(W)$ must equal $\mathbf{0}'$. $\square$

3. The proof of Corollary 1.6

As usual for these arguments, we only have to check that

(i) WKL_0 (or ACA_0, respectively) suffices to prove the existence of a (finite-dimensional) nontrivial proper subspace (establishing the left-to-right direction of Corollary 1.6); and
(ii) the above computability-theoretic arguments can be carried out in RCA_0 (establishing the right-to-left direction of Corollary 1.6).

Part (i) just requires a bit of coding. Using WKL_0, one can code membership in a nontrivial proper subspace W of a vector space V on a binary tree T where one arbitrarily fixes two linearly independent vectors $w, w' \in V$ such that $w \in W$ and $w' \notin W$ is specified. A node $\sigma \in T_W$ is now terminal if the subspace axioms for W are violated along σ using coefficients with Gödel number $< |\sigma|$, which can be checked effectively relative to the open diagram of the vector space. Using ACA_0, one can form the one-dimensional subspace generated by any nonzero vector in V.

Part (ii) boils down to checking that Σ^0_1-induction suffices for the computability-theoretic arguments from Section 2. First of all, note that the definition of U and of the vector space operations on U can be carried out using Δ^0_1-induction. WKL_0 is equivalent to showing Σ^0_1-separation, so fix any sets A and B that are Σ^0_1-definable in our model of arithmetic. Then their enumerations $\{A_s\}_{s\in\omega}$ and $\{B_s\}_{s\in\omega}$ exist in the model, and from them we can define the subspace U, the quotient space $V = V^\infty/U$, and the function mapping each vector $v \in V^\infty$ to its $<_{\mathbb{N}}$-least representative modulo U, using only Σ^0_1-induction. (The latter function only requires that in RCA_0, any infinite Δ^0_1-definable set can be enumerated in order.) The hypothesis now provides the nontrivial proper subspace W, and from it we can define the separating set S by Δ_1^0-induction.

Proving the right-to-left direction of Corollary 1.6(2) could be done using the concept of maximal pairs of c.e. sets as in our companion paper [3]. But for vector spaces, there is actually a much simpler proof: In the above construction, simply set A to be any Σ_1^0-set and $B = \emptyset$. Now V must be a vector space of dimension greater than one. Since any finitely generated nontrivial proper subspace can compute a one-dimensional subspace, we may assume we are given a one-dimensional subspace W, spanned by v_i, say. But then

$$n \in A \text{ iff } \{v_i, e_{g(i,1,n)}\} \text{ is linearly dependent in } V \text{ iff } e_{g(i,1,n)} \in W,$$

and so W can compute A as desired.

References

[1] Marat M. Arslanov, Some generalizations of a fixed-point theorem, Izv. Vyssh. Uchebn. Zaved. Mat. 25 (5) (1981) 9–16, translated in: Soviet Math. (Iz. VUZ) 25 (5) (1981) 1–10.
[2] Jacob C.E. Dekker, Countable vector spaces with recursive operations. I, J. Symbolic Logic 34 (1969) 363–387.
[3] Rodney G. Downey, Steffen Lempp, Joseph R. Mileti, Ideals in computable rings, J. Algebra 314 (2007) 872–887.
[4] George Metakides, Anil Nerode, Recursively enumerable vector spaces, Ann. Math. Logic 11 (1977) 147–171.

Further reading

[5] Carl G. Jockusch Jr., Robert I. Soare, Π_1^0 classes and degrees of theories, Trans. Amer. Math. Soc. 173 (1972) 33–56.
[6] Piergiorgio Odifreddi, Classical Recursion Theory, North-Holland, Amsterdam, 1989.
[7] Piergiorgio Odifreddi, Classical Recursion Theory, vol. II, North-Holland, Amsterdam, 1999.
[8] Stephen G. Simpson, Subsystems of Second Order Arithmetic, Springer-Verlag, Berlin, 1999.
[9] Robert I. Soare, Recursively Enumerable Sets and Degrees, Springer-Verlag, Berlin, 1987.